WM389-15 Network Security

27/28

Department
WMG
Level
Undergraduate Level 3
Module leader
Alaa Al Sebae
Credit value
15
Module duration
14 weeks
Assessment
100% coursework
Study locations
University of Warwick main campus, Coventry Primary
Distance or Online Delivery

Description

Introductory description

The integration of cyber-physical systems and the exponential increase of devices, software and applications increased the security implications that underpin everything we do in cyberspace. Assessing these cyberinfrastructures for security and resilience necessitates hybrid and proactive approaches to help us to enhance our understanding or baselines of our current systems' security resistance. Cyber Defence has become one of the biggest business priorities to deal with dynamic attack vectors while still relying on static controls and measures. It is a systematic approach to help organisations to better articulate, manage and change threat thresholds and improve the effectiveness of security controls. This module seeks to address the core principles, methods, tools, and products available used in proactive cyber operations to prevent cyber-attacks or decrease the time taken to discover them.

This module equips students to better understand the stages and concepts of a cyber-attack contextualized by some of these frameworks. Additionally, the module will equip and allow students to develop a practical understanding, as well as apply a range of tools, techniques and procedures utilised by adversaries and attackers during each phase of a cyber attack in a manner that is both legal and ethical. Core concepts of cyber security (confidentiality, integrity, availability, identity, authentication, freshness, authorisation) will be introduced in the contexts of several, generic asset configurations and potential threats (malware, phishing, social engineering, man-in-

the-middle).

Module web page

Module aims

The module serves as a comprehensive guide, leading the students through the essential concepts of building and evaluating successful and secure network communication platforms with a focus on all strategic, tactical, and operational aspects. The module seeks to address the core principles, methods, tools, and products available used in information gathering and analytics to aid decision-making to prevent targeted cyber-attacks. It also provides an overview of network security mechanisms, tools, and techniques to better articulate approaches in informed cyber defence.

Outline syllabus

This is an indicative module outline only to give an indication of the sort of topics that may be covered. Actual sessions held may differ.

- Cyber Landscape
- Network design and architecture
- Honeypots
- Threat modelling processes
- Network based attacks
- Intrusion and multi-stage attack analysis
- Lockheed Martin Cyber Kill Chain
- Diamond Model
- MITRE ATT&CK
- Active Reconnaissance
- Passive Reconnaissance
- Exploitation Installation Command & Control (C2)
- Legal and Ethical considerations

Learning outcomes

By the end of the module, students should be able to:

- Evaluate the effectiveness of cyber defence frameworks, tools and techniques in identifying and analysing network attacks in diverse organisational contexts. [CITP 2.1.5] [AHEP4 C12]
- Critically analyse the business impact of cyber-attacks and formulate appropriate security technology solutions. [CITP 2.2.6] [AHEP4 C10]
- Correlate cyber-attack analysis frameworks with common attacks in cyberspace by examining the tools, techniques, and procedures used. [CITP 2.1.2]
- Examine and evaluate tools, techniques, and measures to strengthen network security by implementing predefined security baselines in various organizational contexts. [CITP 2.1.8, 2.2.4]

Indicative reading list

Reading lists can be found in Talis

Subject specific skills

This module covers the following Skills based on the latest published DTS DA standard (ST0119):

- Plan, design and manage simple computer networks with an overall focus on the services and capabilities that network infrastructure solutions enable in an organisational context (S12)
- Discover, identify and analyse security threats, attack techniques and vulnerabilities and recommend mitigation and security controls (S40)
- Secure network systems by establishing and enforcing policies, and defining and monitoring access. Support and administer firewall environments in line with IT security policy (S61)
- Investigate security concerns or attacks. For example, Distributed Denial of Service (DDOS), port scanning, assessing key metrics and indicators, evidencing the chosen steps to mitigate (S63)

Also, students will be able to:

- Develop skills and actively be engaged in network security mechanisms, tools and techniques for real-world scenarios.
- Develop an understanding of ethics, risk, governance, and legal aspects of intelligence gathering in cyber security for effective network defence.
- Develop collaborative abilities through practical sessions and seminars to share ideas and tackle network security challenges.
- Develop creative problem-solving skills to address operational information security management challenges, integrating existing knowledge with workplace demands

Transferable skills

Communication skills
Problem-solving
Ethical Awareness
Critical and Analytical Skills
Teamwork and collaboration
Time Management

Study

Study time

Type	Required
Lectures	10 sessions of 1 hour (7%)
Practical classes	10 sessions of 2 hours (13%)
Work-based learning	15 sessions of 1 hour (10%)
Online learning (independent)	5 sessions of 1 hour (3%)
Other activity	5 hours (3%)
Private study	35 hours (23%)
Assessment	60 hours (40%)
Total	150 hours

Private study description

Pre-block exercises given on Moodle.
Post-block problem sets released on Moodle.
Free open source virtual environment in which to conduct experiments

Other activity description

NA

Costs

No further costs have been identified for this module.

Assessment

You must pass all assessment components to pass the module.

Assessment group A2

	Weighting	Study time	Eligible for self-certification
Assessment component			
Coursework	40%	24 hours	Yes (extension)

Students will prepare a written report to assess their understanding of cyber defence frameworks, tools, and techniques within a specific scenario.

Reassessment component is the same

	Weighting	Study time	Eligible for self-certification
Assessment component			
Coursework	60%	36 hours	Yes (extension)

Students will prepare a written report to design a secure network that aligns with the specific requirements of a given network as well as utilize security tools to identify and analyse potential network attacks in the given scenario.

Reassessment component is the same

Feedback on assessment

Feedback is given as appropriate to the assessment type:

- verbal feedback given during seminar/tutorial sessions
- formative feedback on the individual contributions
- written feedback on the final group reports

Availability

Courses

This module is Core for:

- DWMS-H655 Undergraduate Digital and Technology Solutions (Cyber) (Degree Apprenticeship)
  - Year 3 of H655 Digital and Technology Solutions (Cyber) (Degree Apprenticeship)
  - Year 4 of H655 Digital and Technology Solutions (Cyber) (Degree Apprenticeship)
- DWMS-H653 Undergraduate Digital and Technology Solutions (Network Engineering) (Degree Apprenticeship)
  - Year 3 of H653 Digital and Technology Solutions (Network Engineering) (Degree Apprenticeship)
  - Year 4 of H653 Digital and Technology Solutions (Network Engineering) (Degree Apprenticeship)

This module is Optional for:

- DWMS-H652 Undergraduate Digital and Technology Solutions (Data Analytics) (Degree Apprenticeship)
  - Year 3 of H652 Digital and Technology Solutions (Data Analytics) (Degree Apprenticeship)

    - Year 4 of H652 Digital and Technology Solutions (Data Analytics) (Degree Apprenticeship)
- DWMS-H654 Undergraduate Digital and Technology Solutions (Software Engineering) (Degree Apprenticeship)
    - Year 3 of H654 Digital and Technology Solutions (Software Engineering) (Degree Apprenticeship)
    - Year 3 of H654 Digital and Technology Solutions (Software Engineering) (Degree Apprenticeship)
    - Year 4 of H654 Digital and Technology Solutions (Software Engineering) (Degree Apprenticeship)
    - Year 4 of H654 Digital and Technology Solutions (Software Engineering) (Degree Apprenticeship)